REMARKS

In the Office Action, FIGS. 5 and 6 are objected because of improper labeling to the reference characters "515" and "615". Applicant respectfully agrees to the objection and the FIGS. 5 and 6 are amended as suggested.

The Office Action further states that the reference character "429" has been used to designate both "Store Application keys" and "Derive Application Keys." Applicant respectfully agrees and has amended FIG. 4 with a different reference character "428" to designate "Store Application Keys". Also, Applicant has made similar changes in the paragraph that begins on page 18, line 4 of the Application as filed. Applicant therefore respectfully requests to kindly withdraw the objection.

The specification is objected to and suggests are made to amend pages 5, 10, 12 and 20. Applicant respectfully agrees and has made the requested changes. Applicant therefore requests to kindly withdraw the objection.

Claims 11 and 13-20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Applicant disagrees with the Office Action and traverses this rejection as an "application client" is a part of a "system entity" which is used for initiating different applications such as SIP, MIP etc. In particular, "the application client initiates contact with the relevant application server and provides an identity associated with the particular client or user." The system entity includes other structural units such as the key manager, which is shown in FIGS 2 and 3 and key manager 203/303, a L2 authentication client unit and a persistent storage unit.

For example, the L2 authentication client unit authenticates and establishes a network connection with the network. The authentication provides a dynamic seed, which is used by the key manager to generate an application key. The application key is finally used by the

application client unit to facilitate authenticating an application. In addition, the referred phrase "specifically an application client," on page 12 of the Application as filed is actually referring to the last stage, where the application client within the system entity, utilizes the generated application key to initiate contact with the relevant application server. Thus, it is improper to interpret the system entity as the application client composed entirely of software with no structural components. Applicant therefore respectfully requests to kindly withdraw the rejection.

Rejection of Claims 1-9 and 11-19 under 35 U.S.C. § 102 (b) as being anticipated by US 5,745,571 to Zuk

Applicant respectfully traverses the rejection of claims 1-9 and 11-19.

MPEP § 2131 provides: "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Applicant respectfully submits that Zuk does not anticipate, either expressly or inherently, each and every element as set forth in independent claims 1 and 11. Applicant's independent claims 1and 11 require a client "establishing a network connection further comprising an authentication with the network," and "obtaining, responsive to the authentication, a dynamic seed." The client further utilizes the dynamic seed for "generating an application key corresponding to the dynamic seed and providing the application key to facilitate authenticating an application." Applicant's client establishes connection with the network only after successful authentication with the network. Also, the client utilizes the dynamic seed, which was obtained during authentication, for generating an application key. More specifically, Applicant claim a client "obtaining, responsive to the authentication, a dynamic seed" and "generating an

application key corresponding to the dynamic seed" that is not disclosed either expressly or inherently, in Zuk.

Applicant's invention discloses a method of providing authentication services for applications running on a client and requiring access to a network based server where the method uses lower layer keying to provide upper layer security. The method is practiced in corresponding client and network entities. The method comprises establishing a network connection including an authentication with the network; obtaining, responsive to the authentication, a dynamic seed; generating an application key corresponding to the dynamic seed; and providing the application key to facilitate authenticating an application.

Zuk is directed to "storing a random key on the card (6), encrypting the random key on the basis of a public key, and providing the encrypted random key to a central processing station (4)." Thus, Zuk's random key is stored in a smart card and moreover, random key is provided to the central processing station for producing an application key. See abstract of Zuk. On the other hand, Applicant's claim a "dynamic seed," which can be equated to Zuk's "application key," that is obtained by a client in response to an authentication with a network.

Moreover, Applicant respectfully disagrees with the statement regarding claim 11 found on page 6 of the Office Action that Zuk describes a smart card establishing contact with a point of sale and generating a random value r and that this random value is used to create an "application, master or authentication key." In contrast, the cited passage actually discloses a smart card that simply connects and generates a random number, which is being used by Zuk's central processing station to generate the key. Thus, Zuk does not teach Applicant's claim limitation of "complete an authentication with the network, the authentication providing a dynamic seed."

In the Office Action, the Examiner interprets Zuk's "application, master or authentication key" as the claimed dynamic seed. Zuk's "application, master or authentication key" is produced by a central processing station based on the random number received from the smart card. On the other hand, the claimed "dynamic seed" is independently obtained by the client after completing

authentication with the network. Thus, Zuk's keys are exchanged between the smart card and the central processing station, whereas Applicant's keys are generated independently at the client and the server.

Therefore, Zuk does not disclose a client "obtaining, responsive to the authentication, a dynamic seed; generating an application key corresponding to the dynamic seed," as required by independent claim 1. Also, Zuk does not disclose a network function "to establish a network connection and complete an authentication with the network, the authentication providing a dynamic seed," as required by independent claim 11. Instead, Zuk describes a smart card that simply establishes contact with a point of sale and generates a random value. The generated value is further transmitted to the central processing station for creating the "application, master or authentication key."

Further, Applicant respectfully submits that Zuk does not anticipate, either expressly or inherently, each and every element as set forth in dependent claims 3 and 13. Dependent claim 3 requires the further limitation of "generating a plurality of application keys where each of the plurality of keys corresponds to a different application" and claim 13 includes a similar limitation Applicant respectfully disagrees that Zuk's "session keys" are multiple keys created for different applications. The cited passage discloses that the "session keys" are used at different instances or invocations of the same application. In other words, Zuk discloses same application invoked on two different instances of time would result in distinct sessions. On the other hand, Applicant's claims require the limitation of "generating a plurality of application keys where each of the plurality of keys corresponds to a different application."

In view of the foregoing, Applicant respectfully submits that Zuk does not disclose a client that obtains dynamic seed in responsive to the authentication, and generates an application key corresponding to the obtained dynamic seed. Applicant therefore submits that claims 1 and 11 are not anticipated by Zuk. The rejection of claims 1 and 11 under 35 USC 102(b) is improper and should be withdrawn. Applicant requests that claims 1 and 11 now be passed to allowance.

Dependent claims 2-9 depend from, and include all the limitations of independent claim 1, and claims 12-20 depend from, and include all the limitations of independent claim 11. Accordingly, claims 1 and 11are shown to be allowable for the reasons given above. Therefore, Applicant respectfully submit that dependent claims 2-9 and 12-20 are in proper condition for allowance and request that claims 1-9 and 11-19 now be passed to allowance.

Rejection of Claims 1-20 under 35 U.S.C. § 102 (e) as being anticipated by US 7,127,613 to Pabla et al.

Applicant respectfully traverses the rejection of claims 1-20.

Applicant respectfully submits that Pabla does not anticipate, either expressly or inherently, each and every element as set forth in independent claims 1 and 11. As stated above, claims requires a client "establishing a network connection further comprising an authentication with the network," and "obtaining, responsive to the authentication, a dynamic seed," which is not anticipated either expressly or inherently, in Pabla.

Pabla is directed to provide secured sessions between two peers in a peer-to-peer networking environment. If the first peer wants to have a secured session with a second peer, the first peer sends a message including the public key to the second peer. Thus, Pabla's public key is generated only when a secured session is required, and not after completing authentication with a network. Moreover, Pabla's public key is generated in the first peer, but a session key is generated in the second peer based on the public key received from the first peer. Thus, keys are exchanged between the peers in the network. On the other hand, as Applicant's claimed keys are generated independently at the client and the server, there is no requirement to exchange keys between the client and the server. Moreover, Applicant's keys are generated after successful authentication with the network, and not when a secured session is required.

Applicant respectfully disagrees with the statement regarding claims 1 and 11 that Pabla describes "two peers communicating over a network where one peer sends the other a generated public key, and the public key is then used by the second peer to create a session key." Applicant

respectfully submit that the cited passage discloses a first peer generating a public key and a second peer generating a session key based on the received public key. Moreover, keys are generated only when a secured session is required between the first peer and the second peer. On the other hand, Applicant's claim 1 requires the limitation of "obtaining, responsive to the authentication, a dynamic seed" and "generating an application key corresponding to the dynamic seed." Claim 11 requires the limitations of "complete an authentication with the network, the authentication providing a dynamic seed" and "generating an application key corresponding to the dynamic seed."

Further, Applicant respectfully submits that Pabla does not anticipate, either expressly or inherently, each and every element as set forth in dependent claims 3 and 13. Dependent claim 3 requires the further limitation of "generating a plurality of application keys where each of the plurality of keys corresponds to a different application." Applicant respectfully disagrees that Pabla's "session keys" are a plurality of application keys where each application has a different key. The cited passage, discloses that the session keys are related to groups or groups within groups. In other words, Pabla's session keys are not representing a particular application; instead they are representing a group of peers. On the other hand, Applicant's claim requires the limitation of "generating a plurality of application keys where each of the plurality of keys corresponds to a different application."

Applicant respectfully submits that Pabla does not anticipate, either expressly or inherently, each and every element as set forth in dependent claims 7 and 17. Dependent claims 7 and 17 require the further limitation of "obtaining a new dynamic seed each time an authentication with the network occurs." Applicant respectfully disagrees that Pabla teaches this limitation. The cited passage, discloses that the public key is generated each time a secure session is to be established with the other peer. In other words, Pabla's public key is not generated every time the client authenticates itself with the network. On the other hand, Applicant's claim requires the limitation of "obtaining a new dynamic seed each time an authentication with the network occurs."

In view of the foregoing, Applicant respectfully submits that Pabla does not disclose a client that obtains a dynamic seed in responsive to the authentication, and generates an application key corresponding to the obtained dynamic seed. Applicant therefore submits that claims 1 and 11 are not anticipated by Pabla. The rejection of claims 1 and 11 under 35 USC 102(e) is improper and should be withdrawn. Applicant requests that claims 1 and 11 now be passed to allowance.

Dependent claims 2-10 depend from, and include all the limitations of independent claim 1, and claims 12-20 depend from, and include all the limitations of independent claim 11. Accordingly, claims 1 and 11 are shown to be allowable for the reasons given above. Therefore, Applicant respectfully submit that dependent claims 2-9 and 12-20 are in proper condition for allowance and request that claims 1-20 now be passed to allowance.

Applicant respectfully request that a timely Notice of Allowance be issued in this case. Such action is earnestly solicited by the Applicant. Should the Examiner have any questions, comments, or suggestions, the Examiner is invited to contact the Applicant's attorney or agent at the telephone number indicated below.

Please charge any fees that may be due to Deposit Account 502117, Motorola, Inc.

Respectfully submitted,
Chad M. Fors, et al.

SEND CORRESPONDENCE TO:

By: /Simon B. Anolick/

Motorola, Inc.
Law Department

Customer Number: **22917**

Simon B. Anolick
Attorney for Applicant
Registration No.: 37,585
Telephone: 847-576-4234
Fax: 847-576-3750